IFW

Practitioner's Docket No. U 014712-9 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Joost Alexander SPIERENBURG
Serial No.: 10/616,903 Group No.: 2621
Filed: July 10, 2003 Examiner:
For: DIGITAL SECURITY IMAGE PROVIDED WITH DOUBLE-BANDED CODING

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country: NETHERLANDS

Application Number: 1017173

Filing Date: JANUARY 23, 2001

WARNING: "When a document that is required by statute to be certified must be filed, a copy, including a photocopy or facsimile transmission of the certification is not acceptable." 37 C.F.R. 1.4(f) (emphasis added).

CERTIFICATE OF MAILING (37 C.F.R. 1.8a)

I hereby certify that this correspondence is, on the date shown below, being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450.

Signature

Date: AUGUST 10, 2004

WILLIAM R. EVANS
(type or print name of person certifying)

SIGNATURE OF PRACTITIONER

Reg. No. 25858

WILLIAM R. EVANS
(type or print name of practitioner)

Tel. No.: (212) 708-1930

P.O. Address

Customer No.: 00140

c/o Ladas & Parry LLP
26 West 61st Street
New York, N.Y. 10023

NOTE: *"The claim to priority need be in no special form and may be made by the attorney or agent, if the foreign application is referred to in the oath or declaration, as required by § 1.63."* 37 C.F.R. 1.55(a).

SN 10/616 903
GN 2621

KONINKRIJK DER NEDERLANDEN

Bureau voor de Industriële Eigendom

Hierbij wordt verklaard, dat in Nederland op 23 januari 2001 onder nummer 1017173,

ten name van:

JOH. ENSCHEDÉ B.V.

te Haarlem

een aanvrage om octrooi werd ingediend voor:

"Beveiliging voorzien van dubbelbandige codering",

en dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

Rijswijk, 6 augustus 2003

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,

Mw. M.M. Enhus

UITTREKSEL

De uitvinding heeft betrekking op een beveiliging, aan te brengen op een document, zoals waardepapieren of andere documenten waarvan de authenticiteit of herkomst van belang is, voorzien van een eerste beveiligingskenmerk dat bij kopiëren van het document detecteerbaar op een kopie overgenomen wordt en van een tweede beveiligingskenmerk dat bij kopiëren van het document niet overgenomen wordt op een kopie, alsmede een werkwijze voor het aanbrengen en voor het detecteren van een dergelijke beveiliging, alsook programmatuur daarvoor.

Daarnaast heeft de uitvinding betrekking op een afbeelding en een afbeelding in electronische vorm, voorzien van de beveiliging volgens de uitvinding.

Nr. 162 459

Beveiliging voorzien van dubbelbandige codering

De uitvinding heeft betrekking op een beveiliging, aan te brengen op een document, zoals waardepapieren of andere documenten waarvan de authenticiteit of herkomst van belang is.

In de praktijk is het bijvoorbeeld gebruikelijk om een document, al niet voorzien is van een afbeelding, te voorzien van een beveiliging tegen ongeauthoriseerd kopieren. Een dergelijke beveiliging is bijvoorbeeld in de vorm van een beveiligingsafbeelding, waarbij in de afbeelding een beveiligingsafbeelding opgenomen is die niet of nauwelijks door het menselijk oog waar te nemen is.

In het verleden zijn documenten daartoe voorzien van een beveiligingskenmerk dat bij kopiëren verdwijnt van de kopie, waardoor detecteerbaar is of een document authentiek is of een kopie, waarmee mogelijk gefraudeerd is.

Daarnaast zijn in het verleden ook wel documenten voorzien van een beveiligingskenmerk dat bij kopiëren detecteerbaar aanwezig blijft op de kopie. Daardoor is eventueel na te gaan of een kopie afkomstig is van een origineel, of een namaak is.

Als dergelijke kenmerken al tegelijkertijd op één document werden aangebracht, dan werden de verschillende soorten kenmerken tot op heden echter in verschillende afbeeldingen of op verschillende plaatsen op een document aangebracht. Nadeel daarvan is dat de beveiligingskenmerken

daardoor een grote ruimte innemen op een te beveiligen document. Daarnaast vindt detectie van de verschillende kenmerken daardoor gescheiden plaats. Doordat het detecteren van de verschillende kenmerken vaak rekenintensief is, indien het een kenmerk is dat middels specifieke beeldbewerkingstechnieken zichtbaar te maken is, is het daardoor in veel gevallen niet of nauwelijks mogelijk de verificatie real-time uit te voeren, bijvoorbeeld bij een kassa in een winkel. Daarnaast is verificatie van grote aantallen documenten tijdrovend.

Daarnaast is een probleem dat bij de huidige beveiligingen optreedt dat niet aangegeven kan worden of een niet-authentiek document een kopie van een origineel is, of een complete vervalsing, in het bijzonder niet wanneer één beveiligingskenmerk is aangebracht.

De uitvinding heeft tot doel de verschillende nadelen althans gedeeltelijk op te heffen en problemen op te lossen, en voorziet daartoe in een beveiliging, aan te brengen op een document, zoals waardepapieren of andere documenten waarvan de authenticiteit of herkomst van belang is, voorzien van een eerste beveiligingskenmerk dat bij kopiëren van het document detecteerbaar op een kopie overgenomen wordt en van een tweede beveiligingskenmerk dat bij kopiëren van het document niet overgenomen wordt op een kopie.

Door te kiezen voor het voorzien van een beveiliging van ten minste twee beveiligingskenmerken, wordt de mogelijkheid gecreëerd om in één detectieslag beide beveiligingskenmerken te verifiëren. Daarnaast is het mogelijk om een document te creëren dat verschillende veiligheids- of authorisatieniveaus heeft. Er kan namelijk geconstateerd worden of het een authentiek document betreft (eerste groep), een kopie van een authentiek document (tweede groep), of een namaak.

In deze octrooiaanvrage is de term resolutie gebruik voor het onderscheidend vermogen, dus de resolutie in de fysische zin, van opneemapparaten die een fysieke

afbeelding om kunnen zetten in een electronische vorm, zoals een scanner of een digitaal fototoestel of still-video camera of CCD videocamera. Daarnaast is de term resolutie gebruikt voor de zogenaamde dot-pitch van afdruk- of weergave apparaten zoals printers en drukmachines. Er wordt mee bedoelt het aantal punten dat een dergelijk apparaat bijvoorbeeld per cm of inch weer kan geven.

Een document volgens de uitvinding betreft bij voorkeur een document waarvan de authenticiteit van belang is. Bij een document kan ook gedacht worden aan een etiket of label dat op een product is aangebracht of daarin verwerkt is.

Een afbeelding zoals in deze aanvrage gebruikt is heeft betrekking op een kleuren- of grijswaarden foto of tekening, maar kan ook een al dan niet regelmatig, herkenbaar patroon zijn.

Bij voorkeur betreft de uitvinding beveiligingskenmerken die aan een afbeelding toegevoegd zijn die niet of nauwelijks voor het menselijk oog zichtbaar dan wel herkenbaar zijn. Over het algemeen betekent dit bij de huidige technische ontwikkeling dat de resolutie van het beveiligingskenmerk hoger is dan 250 dpi (dots per inch, punten per inch, een gebruikelijke maat om de resolutie van printers en scanners aan te geven). De precieze waarde is afhankelijk van de kleur of kleurcomponent van de afbeelding en de observatieafstand. Voor het menselijk oog ligt dat in de orde van 100 dpi op 30 cm afstand.

Huidige (kleuren) kopieerapparaten hebben over het algemeen een scan/print resolutie van 300-600 dpi. Huidige drukpersen of digitale persen, in het bijzonder voor beveilig drukwerk zoals waardepapieren, kunnen genoemde drukpersen of digitale persen een resolutie hebben van meer dan 10.000 dpi. Volgens de sampling theorie ("bemonsterings theorie") is het originele signaal te reconstrueren wanneer de bemonsteringsfrequentie ten minste twee maal de signaal-frequentie is.

Bij voorkeur betreffen het eerste en het tweede beveiligingskenmerk eerste en tweede afbeeldingen die in het Fourier frequentiedomein aan de amplitude waarden van een afbeelding toegevoegd zijn. Met andere woorden, de beveiligingskenmerken zijn aan het Fourier amplitudespectrum van een originele afbeelding toegevoegd. Hiertoe is één afbeelding toegevoegd in een gebied waarvan de frequenties ligt boven de visuele frequentie maar onder de bemonsteringsfrequentie van bijvoorbeeld een kleurenkopieerapparaat, de tweede afbeelding in een gebied boven de bemonsteringsfrequentie van bijvoorbeeld een kleurenkopieerapparaat.

De Fourier amplitude wordt ook wel beschreven als de lengte van een vector, waarbij de bijbehorende Fourier fase beschreven wordt als de hoek van de bovengenoemde vector. Dit illustreert dus een complex getal.

Bij voorkeur wordt één afbeelding als reële afbeelding in het frequentiedomein bij de Fouriergetransformeerde van originele afbeelding toegevoegd, terwijl van een tweede afbeelding de amplitudes van de Fouriergetransformeerde gespiegeld worden of op een andere wijze omgezet worden naar waarden in een frequentiegebied dat zo min mogelijk invloed uitoefent op de reeds in het frequentiedomein van de originele afbeelding aanwezige waarden en vervolgens bij het amplitudebeeld van de originele afbeelding opgeteld. Met zo min mogelijk invloed uitoefenen wordt hier bedoeld dat in de uiteindelijke afbeelding zoals aangebracht op een document de beide afbeeldingen die aangebracht zijn als beveiligingskenmerk visueel niet of nauwelijks te zien zijn.

Het voordeel van het benutten van het Fourier amplitudespectrum is dat er een directe relatie is tussen de grote van de amplitude in het Fourier frequentiedomein en de resolutie in de reële domein.

Bij voorkeur is de resolutie van de beveiligingskenmerken hoger dan het onderscheidend vermogen van het menselijk oog. Hierdoor is niet zonder hulpmiddelen waar te

nemen dat een document beveiligd is, en wat die beveiliging dan behelst. Daarnaast kan de beveiliging aangebracht worden zonder af te doen aan de esthetische kwaliteit of functionaliteit van de afbeelding. Meer specifiek en bij voorkeur is de resolutie van de beveiligingskenmerken wanneer aangebracht hoger dan 100 dpi.

Het is goed mogelijk gebleken om beveiligingskenmerken aan te brengen die visueel niet of nauwelijks waar te nemen zijn en die bovengenoemde problemen oplossen, door het eerste en tweede beveiligingskenmerk toe te voegen aan het Fourier amplitudespectrum van de originele afbeelding.

Bij voorkeur is het eerste beveiligingskenmerk toegevoegd aan het een eerste frequentiegebied van het Fourier amplitudespectrum van de originele afbeelding, en een tweede beveiligingskenmerk aan een tweede frequentiegebied van het Fourierspectrum van de originele afbeelding.

Bij voorkeur is de originele afbeelding een kleurenafbeelding. Dit heeft als voordeel dat de beveiligingskenmerken in één kleurcomponent of elk in een ander kleurcomponent, bijvoorbeeld in de geel, cyaan of mangenta component of één van de RGB componenten, opgenomen kan zijn. Hierdoor is het beveiligingskenmerk visueel nog moeilijker waar te nemen. Bij voorkeur zijn de beveiligingskenmerken in ten minste één kleurcomponent van de originele afbeelding aangebracht, specifiek verdient het de voorkeur wanneer de beveiligingskenmerken in dezelfde kleurcomponent aangebracht zijn. Hierdoor is het beveiligingskenmerk eenvoudig te detecteren en visueel onzichtbaar te maken. Voor andere redenen kan het echter wenselijk zijn verschillende beveiligingskenmerken in verschillende kleurcomponenten op te nemen.

Bij voorkeur is in een document volgens de uitvinding een eerste beveiligingskenmerk aangebracht in een frequentiegebied van het Fourier amplitudespectrum dat in het plaatsdomein een resolutie heeft van ongeveer 150-600

dpi en een tweede beveiligingskenmerk in een frequentiegebied van het Fourier amplitudespectrum dat in het plaatsdomein een resolutie heeft hoger dan de resolutie van het eerste beveiligingskenmerk. De exacte waarde van de resolutie hangt natuurlijk af van de mogelijkheden van kopieerapparatuur die op de markt is. De gegeven waarden zijn waarden die gelden voor de huidige technische mogelijkheden.

Om een tweede beveiligingskenmerk goed te kunnen reconstrueren verdient het de voorkeur wanneer ook het fasespectrum bij het fasespectrum van een originele afbeelding opgeteld wordt.

De uitvinding heeft daarnaast betrekking op een document voorzien van ten minste een eerste en een tweede beveilingingskenmerk op in hoofdzaak dezelfde plaats op het document, waarbij het eerste beveiligingskenmerk en het tweede beveiligingskenmerk een frequentie hebben hoger dan visueel onderscheidbaar voor het menselijk oog, waarbij verder het eerste beveiligingskenmerk in het Fourier frequentiedomein een frequentie heeft lager dan de print- en scanresolutie van kopieerapparatuur en het tweede beveiligingskenmerk in het Fourier frequentiedomein een frequentie van ten minste twee maal de hoogste van de print- en scanresolutie van kopieerapparatuur.

De uitvinding heeft daarnaast betrekking op een document voorzien van ten minste een eerste en een tweede beveilingingskenmerk op in hoofdzaak dezelfde plaats op het document, waarbij het eerste beveiligingskenmerk in het Fourier frequentiedomein in een gebied ligt dat in het plaatsdomein een frequentie heeft ongeveer tussen 150 en 400 dpi, bij voorkeur ongeveer tussen 250 en 400 dpi, en het tweede beveilingingkenmerk in het Fourier frequentiedomein in een gebied ligt dat in het plaatsdomein een resolutie heeft hoger dan ongeveer 400 dpi, bij voorkeur hoger dan ongeveer 800 dpi.

Bij voorkeur is in het voorgenoemde document het eerste en tweede beveiligingskenmerk aangebracht in het

amplitudespectrum van het Fourier frequentiedomein. Hierdoor is het eenvoudig de beveiligingskenmerken nagenoeg onzichtbaar aan te brengen.

Daarnaast heeft de uitvinding betrekking op een document voorzien van een beveiligde afbeelding, waarbij het amplitudespectrum van de Fouriergetransformeerde van de beveiligde afbeelding een optelling is van het amplitudespectrum van de fouriergetransformeerde van een originele afbeelding, een eerste afbeelding met frequenties in het amplitudespectrum die in het plaatsdomein een resolutie hebben hoger dan 150 dpi en de getransformeerde van het amplitudespectrum van de Fouriergetransformeerde van een tweede afbeelding met frequenties in het amplitudespectrum die in het plaatsdomein een resolutie hebben hoger dan de resoluties van de eerste afbeelding.

Bij voorkeur is in bovengenoemd document de transformatie een laag-doorlaatfilter gevolgd door een transformatie die de lage frequenties omzet maar frequenties boven een drempelwaarde, waarbij de transformaties uitgevoerd worden in het Fourier frequentiedomein.

Bij voorkeur heeft één van de beveiligingskenmerken betrekking op het "Full-Spectrum" kenmerk. Dit kenmerk is uitvoerig beschreven in Developments in digital document security, door S. Spannenburg, Optical Security and Deterrence Techniques III, Volume 3973, page 88-98. Naar dit artikel is hierbij verwezen als ware het volledig in deze tekst opgenomen.

Een tweede beveiligingskenmerk dat bij voorkeur in dezelfde afbeelding opgenomen kan worden als het "full spectrum" beveiligingskenmerk is het beveiligingskenmerk dat aangeduid wordt met SABIC, (Sample Band Image Coding), dat eveneens beschreven is in bovengenoemd artikel van Spannenburg en uitgebreid in WO-A-9527627, dat hierbij middels referentie opgenomen is als ware het volledig ingevoegd in deze tekst. De uitvinding heeft daarnaast betrekking op een werkwijze voor het aanbrengen van beveiligingen op een document, waarbij een eerste beveiligings-

kenmerk met een resolutie hoger dan 100 dpi en een tweede beveiligingskenmerk met een resolutie hoger dan de resolutie van het eerste beveiligingskenmerk en hoger dan van een weergaveapparaat in een originele afbeelding aangebracht wordt. In verband met de voorgenoemde sampling theorie bij voorkeur ten minste twee maal zo hoog als de resolutie van een weergaveapparaat. Een dergelijk weergaveapparaat kan een beeldscherm zijn, bij voorkeur echter een (kleuren) kopieerapparaat, of een combinatie van een scanner met printer. In de praktijk is tot op heden de resolutie van een printer lager dan van beeldopname apparaten, zoals een scanner. De resolutie van de printer zal in dat geval bepalend zijn.

De uitvinding heeft daarnaast betrekking op een werkwijze voor het detecteren van een beveiligingskenmerk zoals hierboven uiteengezet, waarbij een afbeelding omgezet wordt in een in een computer verwerkbare representatie, in het computergeheugen geladen programmatuur een hoogdoorlaatfilter bewerking en een diodefunctie-bewerking op de representatie toepast, en het resultaat vergelijkt, bijvoorbeeld middels een XOR operatie, met een computer verwerkbare representatie van de eerste beveiligingsafbeelding, de Fouriergetransformeerde van de representatie berekent, en het amplitudespectrum vergelijkt met de tweede beveiligingsafbeelding.

De uitvinding heeft daarnaast betrekking op een inrichting voor het detecteren van beveiligingskenmerken in een document of een afbeelding op een document, voorzien van een opnameapparaat voor het opnemen van een beeld van het document of de afbeelding in een voor een computer verwerkbare vorm, een computer verbonden met de opnameapparaat, middelen voor het versturen van het beeld van het opnameapparaat naar een met het opnameapparaat verbonden computer, welke computer voorzien is van een geheugen, een rekeneenheid voorzien van programmatuur voor het berekenen van de Fourier getransformeerde van het beeld in het geheugen, en weergavemiddelen voor het weergeven van een

waardering van de authenticiteit van de afbeelding of het document.

De uitvinding heeft daarnaast betrekking op een afbeelding voorzien van een eerste en tweede beveiligingskenmerk, kennelijk geschikt als beveiligde afbeelding zoals hierboven beschreven.

De uitvinding heeft daarnaast betrekking op een afbeelding in de vorm van een voor een computer verwerkbare vorm op een digitale informatiedrager of in een computergeheugen, voorzien van een eerste en tweede beveiligingskenmerk, kennelijk geschikt als beveiligde afbeelding zoals hierboven beschreven.

De uitvinding heeft daarnaast betrekking op programmatuur, kennelijk geschikt voor het aanbrengen en detecteren van een eerste en tweede beveiligingskenmerk zoals hierboven beschreven.

De uitvinding heeft daarnaast betrekking op een drager voorzien van programmatuur voor de besturing van een computer, kennelijk geschikt voor het uitvoeren van één van de hierboven genoemde werkwijzen.

De uitvinding heeft daarnaast betrekking op een computer, voorzien van een geheugen geladen met programmatuur, kennelijk geschikt voor het uitvoeren van één van de hierboven beschreven werkwijzen.

De uitvinding wordt nader toegelicht aan de hand van een uitvoeringsvoorbeeld volgens de uitvinding. Hierin wordt getoond in:

Figuur 1 een te beveiligen afbeelding,

figuur 2 een amplitude spectrum van de Fourier-getransformeerde (FFT) van figuur 1,

figuur 3 een fase spectrum van de Fouriergetransformeerde (FFT) van figuur 1,

figuur 4 een tweede beveiligingsafbeelding,

figuur 5 Het codebeeld van figuur 4,

figuur 6 het codebeeld, identiek aan figuur 5,

figuur 7 de originele afbeelding,

figuur 8 de som van figuur 6 en 7,

figuur 9 de Fouriergetransformeerde (FFT) van figuur 7, amplitude weergave,

figuur 10 de Fouriergetransformeerde (FFT) van figuur 6, gespiegeld.

figuur 11 de optelling van figuur 9 en 10,

figuur 12 een eerste beveiligingsafbeelding,

figuur 13 Identiek aan figuur 9,

figuur 14 de som van figuur 12 en 13,

figuur 15 identiek aan figuur 1 en 7,

figuur 16 de Fouriergetransformeerde (FFT) van figuur 14,

figuur 17 de diverse amplitude frequentiegebieden in het Fourier (FFT) spectrum,

figuur 18 een originele, te beveiligen afbeelding,

figuur 19 een toe te passen tweede beveiligingsafbeelding,

figuur 20 figuur 18 voorzien van tweede beveiligingskenmerk,

figuur 21 tweede beveiligingsafbeelding zoals gedetecteerd uit figuur 20,

figuur 22 de Fouriergetransformeerde (amplitude plot) van figuur 20,

figuur 23 een eerste beveiligingsafbeelding,

figuur 24 figuur 18 voorzien van eerste en tweede beveilingingskenmerk,

figuur 25 tweede beveiligingsafbeelding zoals gedetecteerd uit figuur 24, en

figuur 26 de Fouriergetransformeerde (amplitude plot) van figuur 24.

figuur 27 stroomschema van de creatie van een afbeelding voorzien van twee beveiligingskenmerken volgens de uitvinding,

figuur 28 stroomschema van de detectie en verwerking,

De figuren komen in enkel gevallen dubbel voor. Dit dient echter ter verduidelijking.

Figuren 1-3 tonen naast elkaar een te beveiligen afbeelding (fig.1), een tweedimensionale afbeelding van het Fourier amplitude spectrum, verkregen door het Fast Fourier Transform (FFT) algoritme toe te passen op figuur 1 (fig. 2), en een tweedimensionale afbeelding van het Fourier fase spectrum, verkregen door toepassing van het FFT algoritme op afbeelding 1.

Figuren 4 toont een tweede beveiligingsafbeelding, en figuur 5 toont de bewerkte tweede beveiligingsafbeelding in een vorm die bij een originele afbeelding opgeteld kan worden. Hiertoe is de Fouriergetransformeerde berekend, op het amplitude spectrum is een laag-doorlaat filter toegepast, en vervolgens is het resultaat gespiegeld, waarbij elk kwadrant gespiegeld is in een diagonaal die het kwadrant in tweeën deelt, maar ook andere bewerkingen waarmee de lage frequenties omgezet worden in hoge frequenties, zoals spiegelingen maar ook andere bewerkingen, zijn denkbaar en toepasbaar. Dit getransformeerde beeld is weer terug getransformeerd middels Fouriertransformatie naar het plaatsdomein.

Figuren 6-8 tonen achtereenvolgens in figuur 6 het bewerkte beeld, identiek aan figuur 5, in figuur 7 de originele, te beveiligen afbeelding identiek aan figuur 1, en in figuur 8 een optelling van figuur 6 en 7.

De figuren 9-11 tonen achtereenvolgens in figuur 9 het amplitude spectrum van de Fourier getransformeerde van figuur 7, in figuur 10 het amplitude spectrum van de Fourier getransformeerde van figuur 6, en in figuur 11 het amplitude spectrum van de Fourier getransformeerde van figuur 8.

De Figuren 12-16 tonen allereerst in figuur 12 een beveiligingsafbeelding, in figuur 13 het amplitudespectrum van de Fouriergetransformeerde van de te beveiligen afbeelding (Rembrandt van figuur 1 en 7), en in figuur 14 de som van figuur 12 en 13. In figuur 15 is ter vergelijk weer de originele, te beveiligen afbeelding getoond, en in figuur 16 de terug getransformeerde van figuur 14. Bij het Fourier

amplitudespectrum van figuur 15 is figuur 12 opgeteld. Visueel is dit nauwelijks waar te nemen (zie figuur 16).

In figuur 17 is het principe te zien van de beveiliging volgens de uitvinding. Hierbij is het Fourier amplitudespectrum weergegeven van de originele afbeelding met eerste en tweede beveiliging. Het Fourier amplitudespectrum is in dit geval opgedeeld in drie gebieden A, B en C. In gebied C bevinden zich de hoofdzakelijke amplitudecomponenten van de originele afbeelding. In frequentiegebied B is een eerste beveiliging aangebracht. De frequentie is dusdanig dat de deze beveiliging bij kopiëren middels een gewoon (eventueel kleuren) kopieerapparaat behouden blijft. In frequentiegebied A is een tweede beveiliging aangebracht met een dusdanige frequentie dat de informatie bij kopiëren middels een gewoon (eventueel kleuren) kopieerapparaat verloren zal gaan. In de figuur is aangegeven dat de grenzen van de gebieden gekozen kan worden. Het is zelfs mogelijk meerdere gebieden te definiëren, bijvoorbeeld op een dusdanige wijze dat gebieden ontstaan waarbij de afbeelding niet meer zichtbaar is in een kopie van een kopie, enzovoorts.

In de figuren 18-26 zijn de reeds getoonde figuren nogmaals weergegeven, maar dan vergroot weergegeven, waardoor details beter zichtbaar zijn.

Zo toont figuur 18 de originele, te beveiligen afbeelding, in dit geval een ets van een zelfportret van Rembrandt. Figuur 19 toont een tijgerkop die gebruikt is als een beveiligingsafbeelding. Figuur 20 toont de afbeelding van figuur 18 waaraan een SABIC codebeeld, dat wil zeggen een bewerkte beveiligingsafbeelding die aan een originele afbeelding toegevoegd kan worden, is toegevoegd, hier de tijgerkop van figuur 19. Figuur 21 toont de tijgerkop zoals die uit figuur 20 te detecteren is. Bij voorkeur gebeurt dat door figuur 20 te scanner met een scanner, en de electronische afbeelding middels de computer en software te bewerken.

Figuur 22 toont het amplitude spectrum van de Fourier getransformeerde van figuur 21. Te zien is centraal de frequenties van het originele beeld, figuur 18, en in de hoeken de gespiegelde frequenties van figuur 19.

Figuur 23 toont een eerste beveiligingsbeeld dat aan figuur 18 toegevoegd kan worden. Deze afbeelding is als Fourier amplitudespectrum gekozen en wordt bij het Fourier amplitudespectrum van figuur 20 opgeteld. In figuur 24 is het resultaat van deze optelling in het plaatsdomein te zien: De originele afbeelding van figuur 18 met in het Fourier amplitudedomein figuur 23 en de getransformeerde van figuur 19 opgeteld.

In figuur 25 is vervolgens de gedetecteerde (SABIC) afbeelding uit figuur 24 te zien. Door de diverse filteringen en transformaties zijn veel details weggevallen, maar de afbeelding is als zodanig nog duidelijk detecteerbaar.

Figuur 26 is de (FFT) Fourier getransformeerde van figuur 24.

Figuur 27 toont het stroomdiagram van de creatie van een beveiligde afbeelding volgens de uitvinding, zoals bijvoorbeeld geïmplementeerd in computer programmatuur. Het stroomschema loopt door op twee bladzijden. Hierbij wordt eerste een beveiligingsafbeelding aangebracht volgens het SABIC principe zoals beschreven in EP-A-328173. Aan de aldus verkregen afbeelding wordt een tweede beveiligingsafbeelding toegevoegd door toevoeging van een afbeelding in het Fourier amplitudedomein, en vervolgens inverse Fouriertransformatie.

Volgens het aangegeven stroomschema wordt eerst een grijswaarden beeld verschaft als tweede beveiligingskenmerk beeld. Van het grijswaardenbeeld worden de grijswaarden teruggebracht van grijswaarden tussen de 0-255 naar waarden van 64-200. Het dynamisch bereik wordt dus verkleind. Daarna wordt de bewerking toegepast die bekend is onder de naam SABIC. Dat wil zeggen dat eerst de Fouriergetransformeerde berekend wordt. Daarna wordt op het amplitu-

despectrum een laagdoorlaatfilter toegepast waardoor de hoge amplitudes weggefilterd worden. Daarna worden de overgebleven amplitudes omgezet naar hogere waarden door een omkeerbare transformatie, bij voorkeur worden de waarden in elk kwadrant gespiegeld, met als resultaat de amplitude weergave van figuur 10. De amplitudes van figuur 10 worden met de originele fasen middels inverse Fourier-transformatie teruggetransformeerd. Een op een te beveiligen afbeelding of een afbeelding die wordt gebruikt om te beveiligen wordt eerste een laag-doorlaat filter toegepast. Bij het resulterende beeld wordt, bij voorkeur 1 op 1, het eerstgenoemde beeld, verkregen met de SABIC methode, opgeteld. Hiermee is de afbeelding dus voorzien van een beveiligingskenmerk dat volgend de uitvinding aangegeven is als het tweede beveiligingskenmerk.

De resulterende afbeelding met tweede beveiligingskenmerk wordt vervolgens getransformeerd met behulp van een Fouriertransformatie, waarna bij het amplitudebeeld een afbeelding, bijvoorbeeld figuur 12, opgeteld wordt. Vervolgens wordt een inverse Fouriertransformatie toegepast. Hiermee is de afbeelding dus additioneel voorzien van het eerste beveiligingskenmerk volgens de uitvinding.

De beschreven procedure kan natuurlijk ook toegepast worden op één of meer, desgewenst verschillende, kleuren waaruit een kleurenbeeld is opgebouwd.

In figuur 28 is een implementatie van de detectie van de verschillende beveiligingsniveaus aangegeven in een stroomschema. Deze detectie is daarbij bij voorkeur geïmplementeerd in computer programmatuur. Hierbij is duidelijk te zien dat in één verificatieslag zowel is aan te geven of het document authentiek is, dan wel een eerste kopie van een authentiek document, dan wel een complete vervalsing. Als invoerafbeelding wordt bijvoorbeeld een beveiligde afbeelding verkregen volgens de methode van figuur 27 toegepast. Allereerst wordt "envelope detectie" toegepast op de invoerafbeelding. Hieruit kan het tweede beveiligingskenmerk verkregen worden. De afbeelding wordt

vergeleken met de afbeelding die oorspronkelijk als tweede beveiliging zou zijn toegevoegd. De programmatuur is voorzien van een beslis-algoritme waaruit een indicatie volgt of de invoer bestaat uit een origineel.

Vervolgens wordt op de invoerafbeelding een Fouriertransformatie toegepast. Het amplitudebeeld wordt vervolgens vergeleken met een afbeelding die als eerste beveiligingskenmerk aan een afbeelding is toegevoegd, en middels een beslis-algoritme volgt een indicatie of de invoerafbeelding gebaseerd is op een originele, authentieke afbeelding, dat wil zeggen of het een kopie kan zijn van een authentieke afbeelding.

Het is natuurlijk mogelijk dat het document zoals boven beschreven een etiket of label of dergelijke is, dat aangebracht is op een voorwerp. Daarnaast kan ook bijvoorbeeld een Compact disk of andere informatiedrager voorzien zijn van een beveiligde afbeelding volgens de uitvinding in digitale vorm.

C O N C L U S I E S

1. Beveiliging, aan te brengen op een document, zoals waardepapieren of andere documenten waarvan de authenticiteit of herkomst van belang is, voorzien van een eerste beveiligingskenmerk dat bij kopiëren van het document detecteerbaar op een kopie overgenomen wordt en van een tweede beveiligingskenmerk dat bij kopiëren van het document niet overgenomen wordt op een kopie.

2. Beveiliging volgens conclusie 1, waarbij de resolutie van de beveiligingskenmerken hoger is dan het onderscheidend vermogen van het menselijk oog.

3. Beveiliging volgens conclusie 2, waarbij de resolutie van de beveiligingskenmerken hoger is dan 100 dpi.

4. Beveiliging volgens één der voorgaande conclusies, waarbij een afbeelding of een deel van een afbeelding het eerste en het tweede beveiligingskenmerk visueel nagenoeg onzichtbaar omvat.

5. Beveiliging volgens één of meer der voorgaande conclusies, waarbij het eerste en tweede beveiligingskenmerk toegevoegd zijn aan het Fourier amplitudespectrum van de originele afbeelding.

6. Beveiliging volgens conclusie 5, waarbij het eerste beveiligingskenmerk toegevoegd is aan het een eerste frequentiegebied van het Fourier amplitudespectrum van de originele afbeelding, en een tweede beveiligingskenmerk aan een tweede frequentiegebied van het Fourierspectrum van de originele afbeelding.

7. Beveiliging volgens conclusie 5 of 6, waarbij een Fourier amplitudespectrum van het tweede beveiligingskenmerk toegevoegd is aan het Fourier amplitudespectrum van de originele afbeelding, en Fourier fasespectrum van het

tweede beveiligingskenmerk toegevoegd is aan het Fourier fasespectrum van de originele afbeelding.

8. Beveiliging volgens één of meer der voorgaande conclusies, waarbij de originele afbeelding een kleurenafbeelding is.

9. Beveiliging volgens conclusie 8, waarbij de beveiligingskenmerken in ten minste één kleurcomponent van de originele afbeelding aangebracht zijn.

10. Beveiliging volgens conclusie 9, waarbij de beveiligingskenmerken in dezelfde kleurcomponent aangebracht zijn.

11. Beveiliging volgens één of meer der voorgaande conclusies, waarbij een eerste beveiligingskenmerk aangebracht in een frequentiegebied van het Fourier amplitudespectrum dat in het plaatsdomein een resolutie heeft van ongeveer 150-600 dpi en een tweede beveiligingskenmerk in een frequentiegebied van het Fourier amplitudespectrum dat in het plaatsdomein een resolutie heeft hoger dan de resolutie van het eerste beveiligingskenmerk.

12. Beveiliging voorzien van ten minste een eerste en een tweede beveilingingskenmerk op in hoofdzaak dezelfde plaats op het document, waarbij het eerste beveiligingskenmerk en het tweede beveiligingskenmerk een frequentie hebben hoger dan visueel onderscheidbaar voor het menselijk oog, waarbij verder het eerste beveiligingskenmerk in het Fourier frequentiedomein een frequentie heeft lager dan de hoogste van de print- en scanresolutie van kopieerapparatuur en het tweede beveiligingskenmerk in het Fourier frequentiedomein een frequentie van ten minste twee maal de hoogste van de print- en scanresolutie van kopieerapparatuur.

13. Beveiliging voorzien van ten minste een eerste en een tweede beveilingingskenmerk op in hoofdzaak dezelfde plaats op het document, waarbij het eerste beveiligingskenmerk in het Fourier frequentiedomein in een gebied ligt dat in het plaatsdomein een frequentie heeft tussen 150 en 400 dpi, bij voorkeur tussen 250 en 400 dpi, en het tweede

beveilingingkenmerk in het Fourier frequentiedomein in een gebied ligt dat in het plaatsdomein een resolutie heeft hoger dan 400 dpi, bij voorkeur hoger dan 800 dpi.

14. Beveiliging volgens conclusie 13, waarbij het eerste en tweede beveiligingskenmerk aangebracht zijn in het amplitudespectrum van het Fourier frequentiedomein.

15. Beveiliging voorzien van een beveiligde afbeelding, waarbij het amplitudespectrum van de Fouriergetransformeerde van de beveiligde afbeelding een optelling is van het amplitudespectrum van de fouriergetransformeerde van een originele afbeelding, een eerste afbeelding met frequenties in het amplitudespectrum die in het plaatsdomein een resolutie hebben hoger dan 150 dpi en de getransformeerde van het amplitudespectrum van de Fouriergetransformeerde van een tweede afbeelding met frequenties in het amplitudespectrum die in het plaatsdomein een resolutie hebben hoger dan de resoluties van de eerste afbeelding.

16. Beveiliging volgens conclusie 15, waarbij de transformatie een laag-doorlaatfilter gevolgd door een transformatie die de lage frequenties omzet maar frequenties boven een drempelwaarde, waarbij de transformaties uitgevoerd worden in het Fourier frequentiedomein.

17. Werkwijze voor het aanbrengen van beveiligingen op een document, waarbij een eerste beveiligingskenmerk met een resolutie hoger dan 100 dpi en een tweede beveiligingskenmerk met een resolutie hoger dan de resolutie van het eerste beveiligingskenmerk en hoger dan van een weergaveapparaat in een originele afbeelding aangebracht wordt.

18. Werkwijze voor het detecteren van een beveiligingskenmerk volgens één of meer der voorgaande conclusies, waarbij een afbeelding omgezet wordt in een representatie die in een computer verwerkbaar is, in het computergeheugen geladen programmatuur een hoogdoorlaatfilter bewerking en een diodefunctie-bewerking op de representatie toepast, en het resultaat vergelijkt met een computer verwerkbare representatie van de eerste beveiligingsafbeelding, de Fouriergetransformeerde berekent van representatie

berekend, en het amplitudespectrum vergelijkt met de tweede beveiligingsafbeelding.

19. Inrichting voor het detecteren van beveiligingskenmerken in een document of een afbeelding op een document, voorzien van een opnameapparaat voor het opnemen van een beeld van het document of de afbeelding in een voor een computer verwerkbare vorm, een computer verbonden met de opnameapparaat, middelen voor het versturen van het beeld van het opnameapparaat naar een met het opnameapparaat verbonden computer, welke computer voorzien is van een geheugen, een rekeneenheid voorzien van programmatuur voor het berekenen van de Fourier getransformeerde van het beeld in het geheugen, en weergavemiddelen voor het weergeven van een waardering van de authenticiteit van de afbeelding of het document.

20. Afbeelding voorzien van een eerste en tweede beveiligingskenmerk, kennelijk geschikt als beveiligde afbeelding volgens één of meer der voorgaande conclusies.

21. Afbeelding in de vorm van een voor een computer verwerkbare vorm op een digitale informatiedrager of in een computergeheugen, voorzien van een eerste en tweede beveiligingskenmerk, kennelijk geschikt als beveiligde afbeelding volgens één of meer der voorgaande conclusies.

22. Programmatuur, kennelijk geschikt voor het aanbrengen en detecteren van een eerste en tweede beveiligingskenmerk volgens één of meer der voorgaande conclusies.

23. Drager voorzien van programmatuur voor de besturing van een computer, kennelijk geschikt voor het uitvoeren van de werkwijze volgens één of meer der voorgaande conclusies.

24. Computer, voorzien van een geheugen geladen met programmatuur, kennelijk geschikt voor het uitvoeren van de werkwijze volgens één of meer der voorgaande conclusies.

25. Drager, zoals een document, voorzien van een beveiligingsinrichting volgens één der voorgaande conclusies.

26. Inrichting omvattend een of meer van de in de beschrijving omschreven en/of in de tekeningen weergegeven kenmerkende maatregelen.

27. Werkwijze omvattend een of meer van de in de beschrijving omschreven en/of in de tekeningen weergegeven kenmerkende maatregelen.

-o-o-o-o-o-o-o-o-o-

PvE

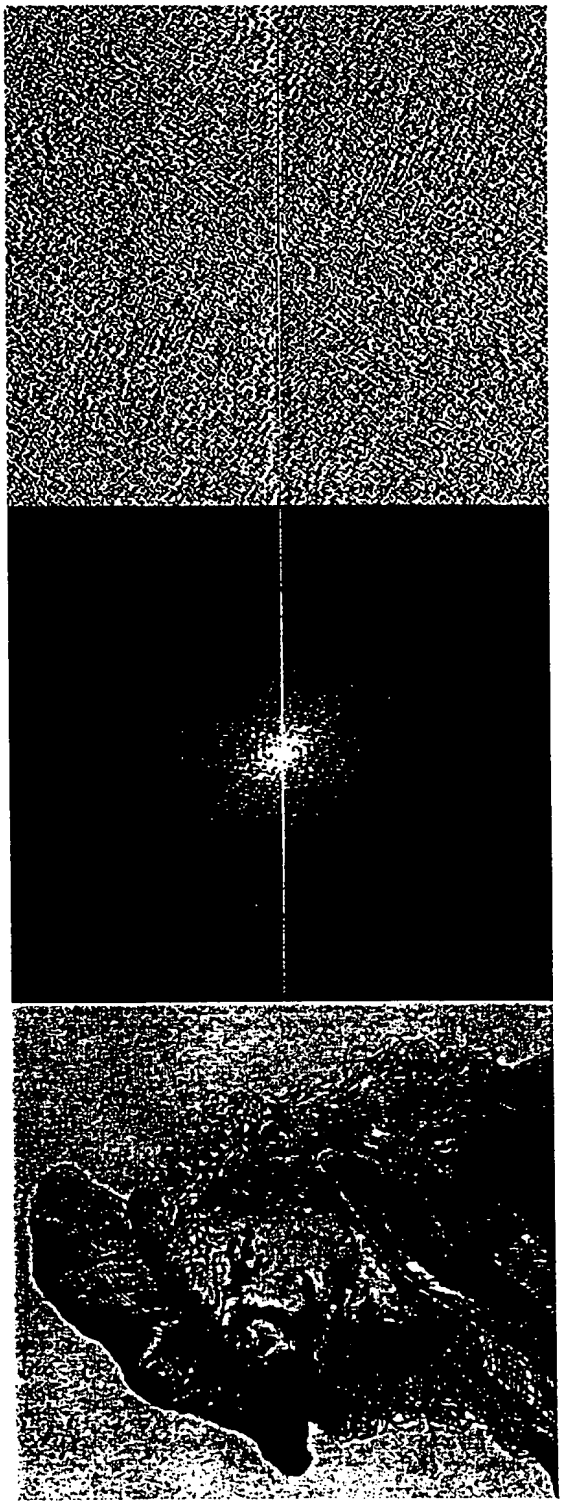

FIG. 3

FIG. 2

FIG. 1

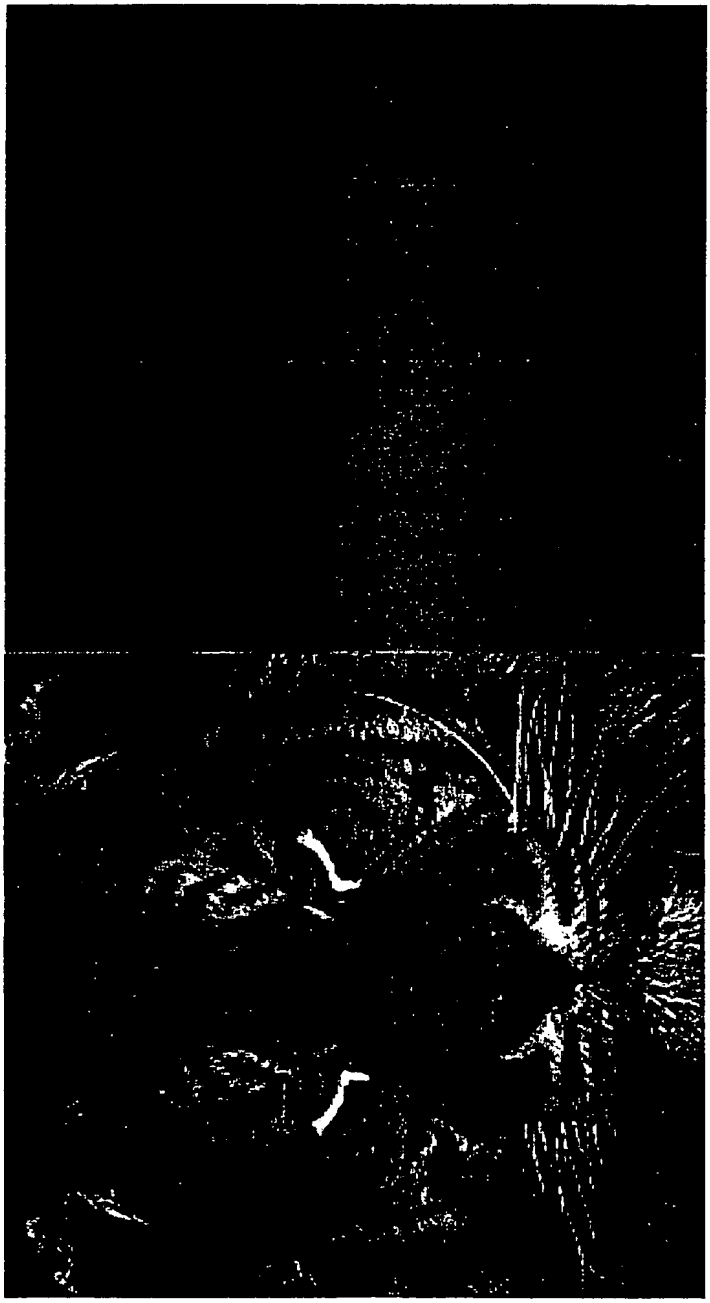

FIG.5

FIG. 4

FIG.8

FIG. 7

FIG. 6

FIG. 9

FIG. 10

FIG. 11

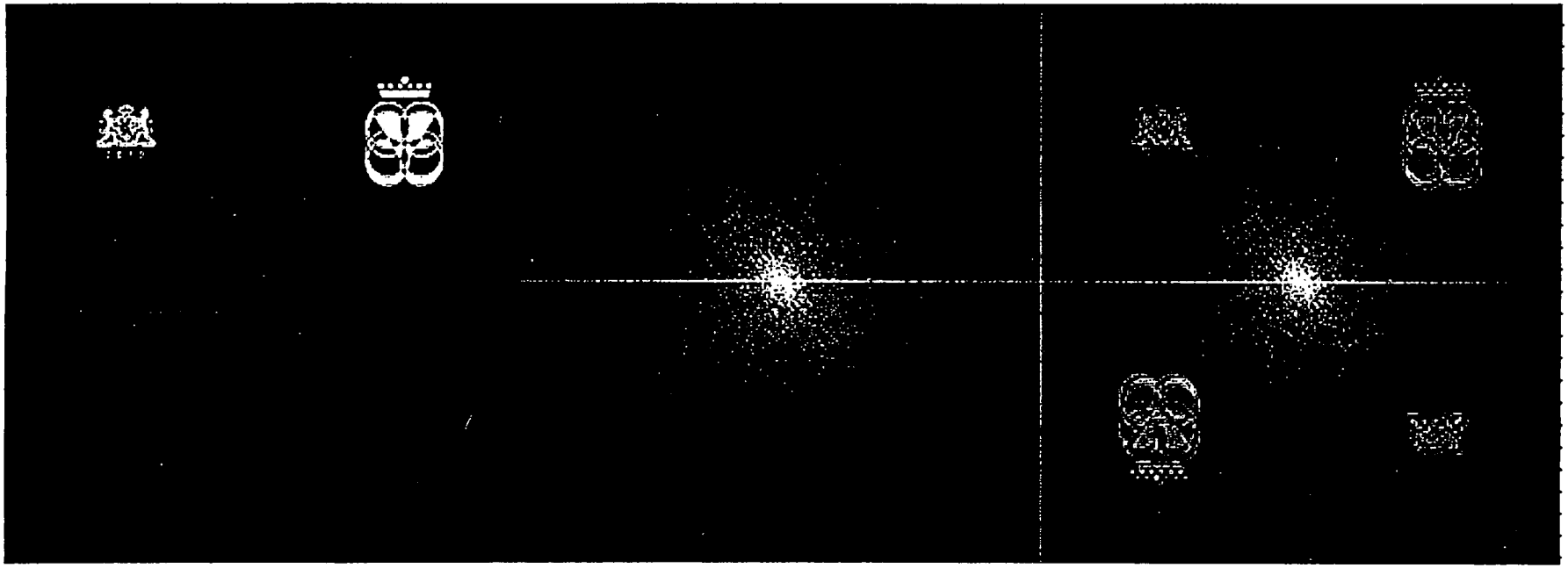

FIG. 12

FIG. 13

FIG. 14

FIG. 15

FIG. 16

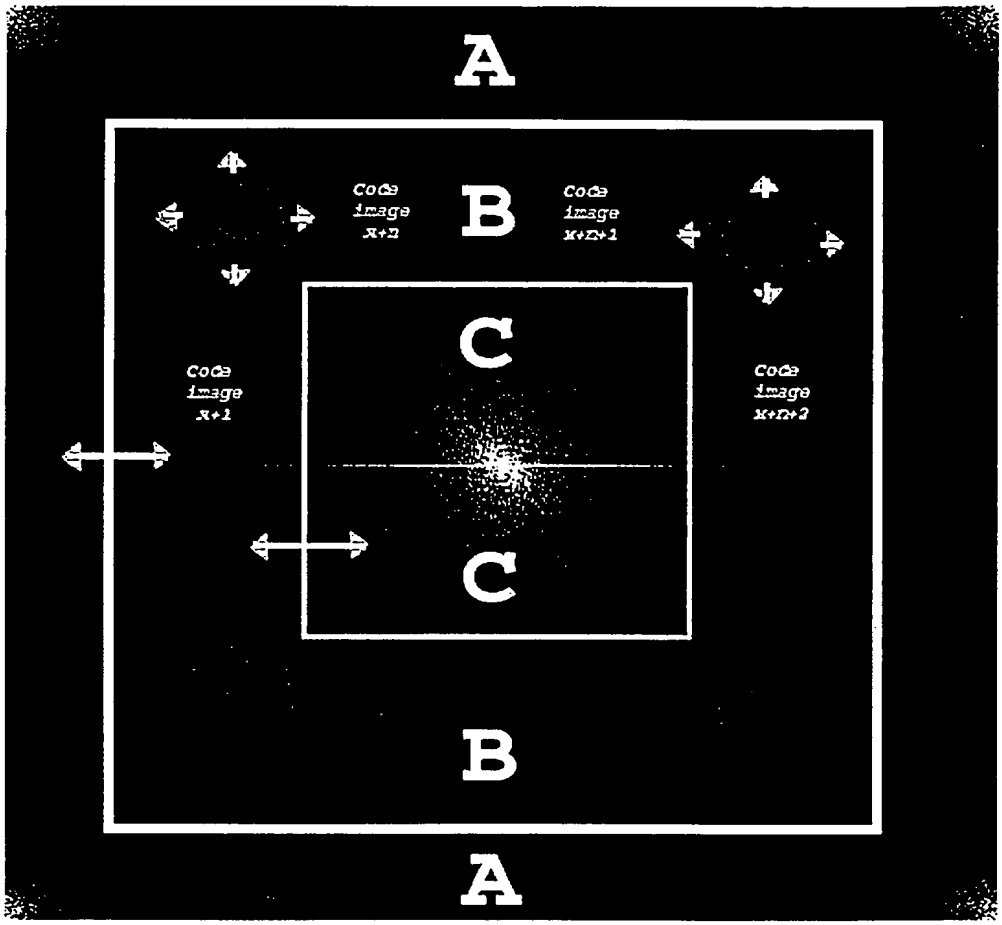
A
B
Code image x+2
Code image x+n+1
C
Code image x+1
Code image x+n+2
C
B
A

FIG. 17

FIG. 18

FIG. 19

FIG. 20

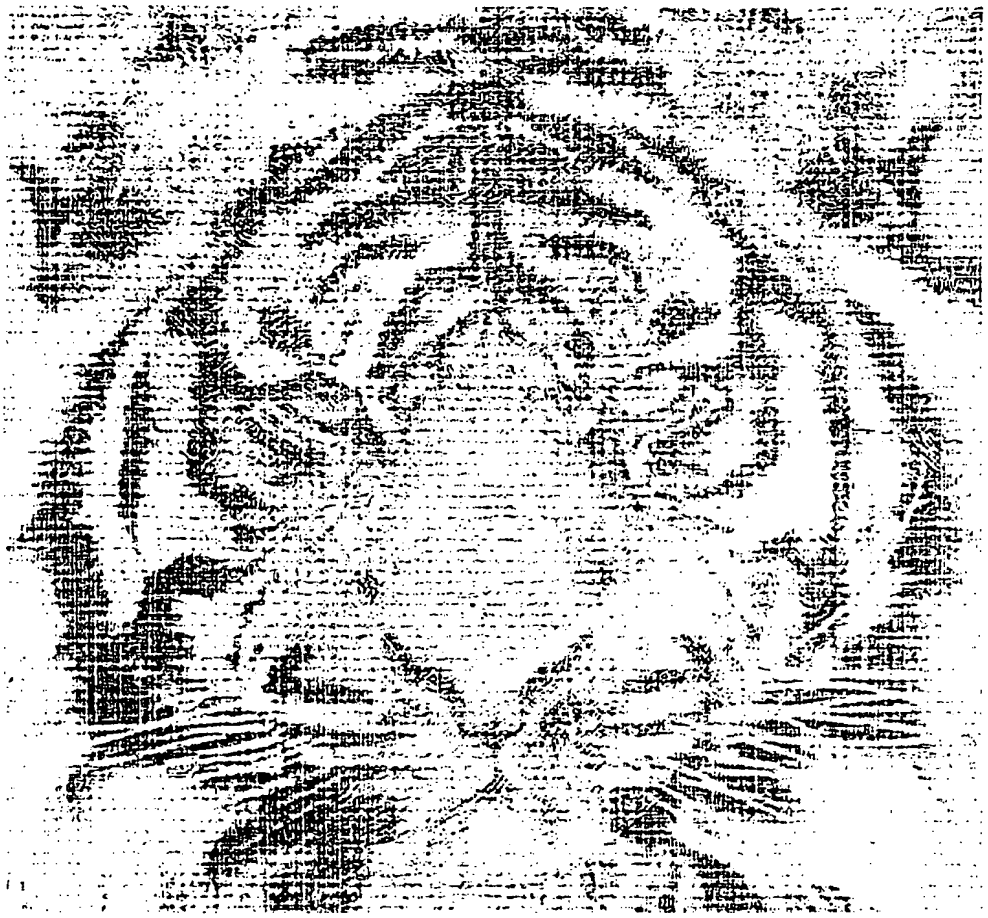

FIG. 21

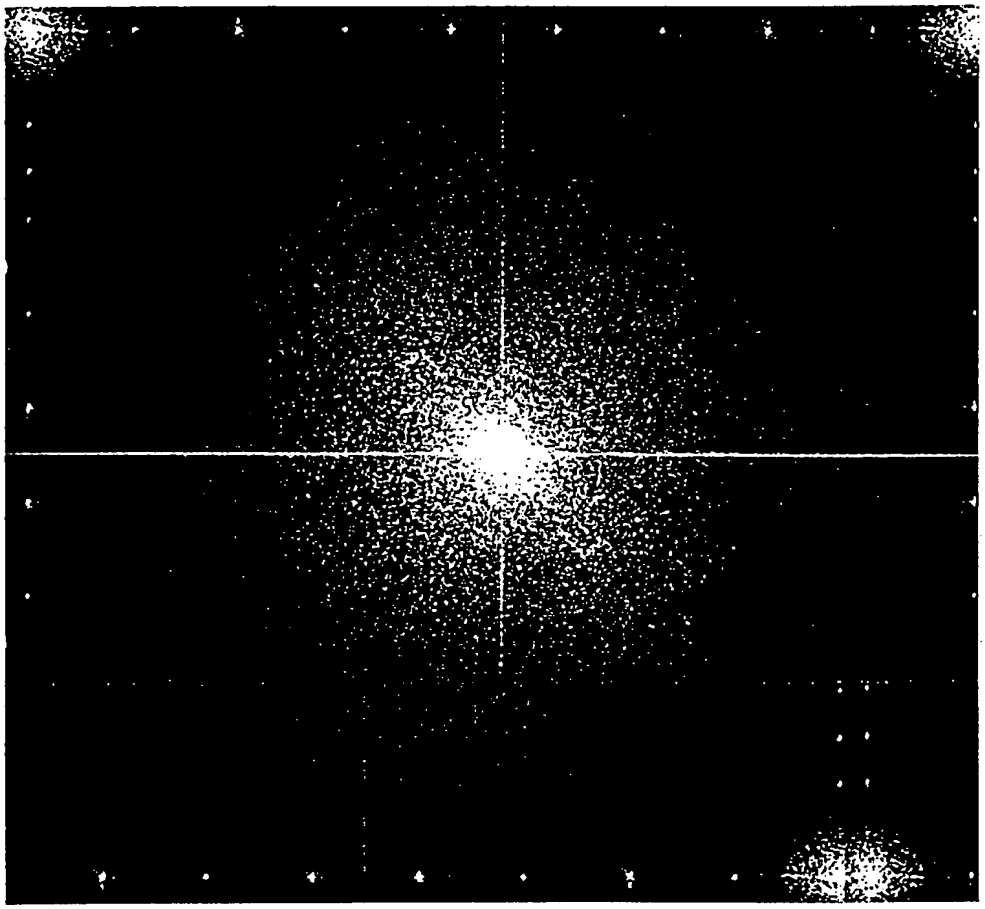

FIG. 22

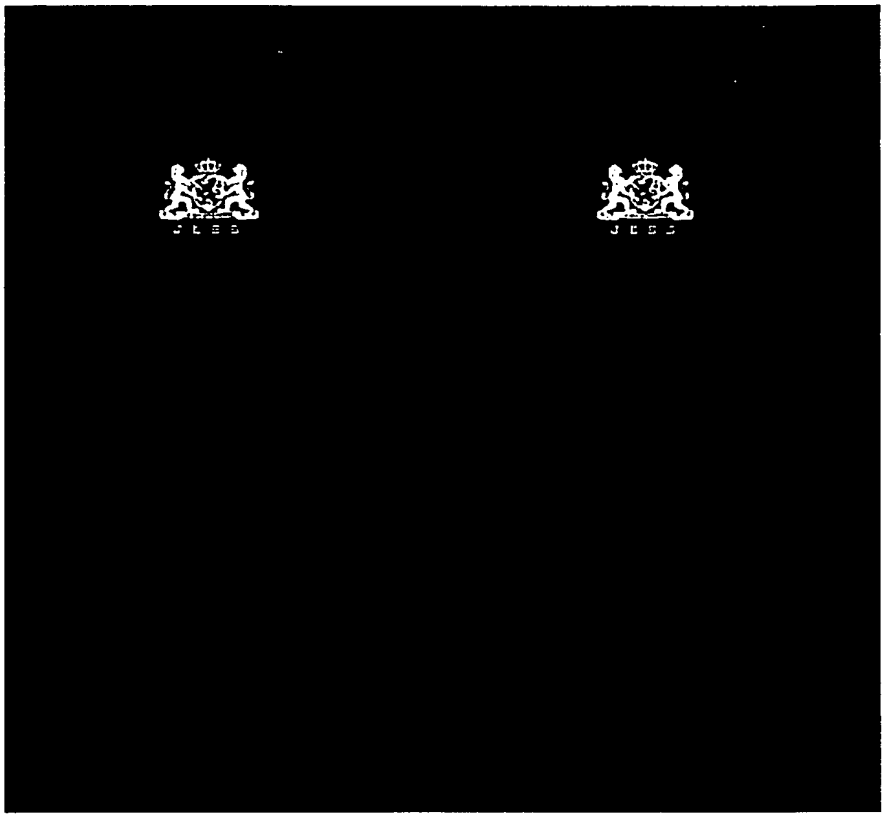

FIG. 23

FIG. 24

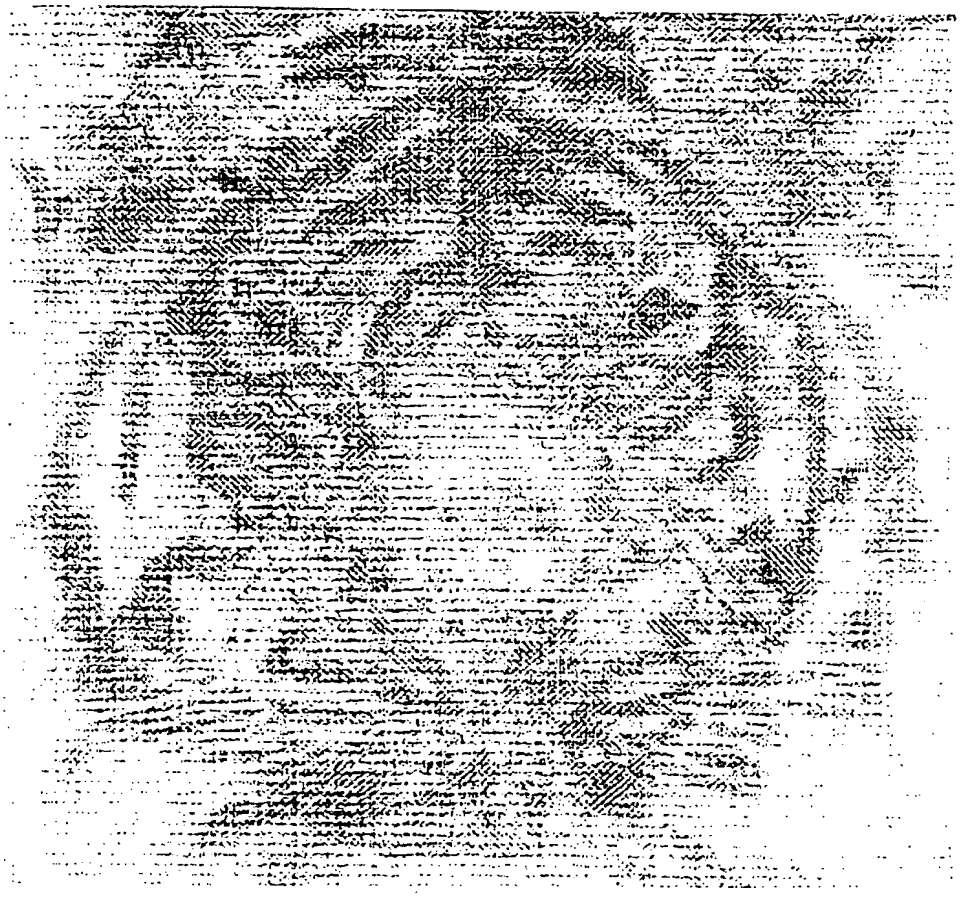

FIG. 25

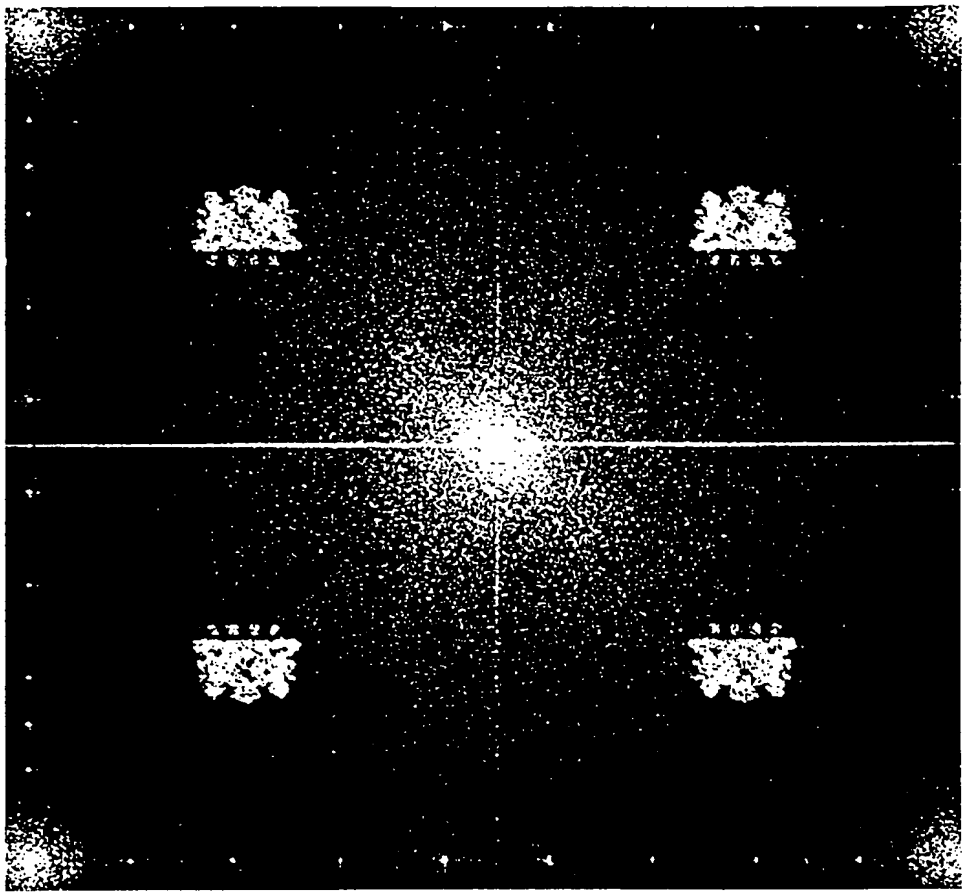

FIG. 26

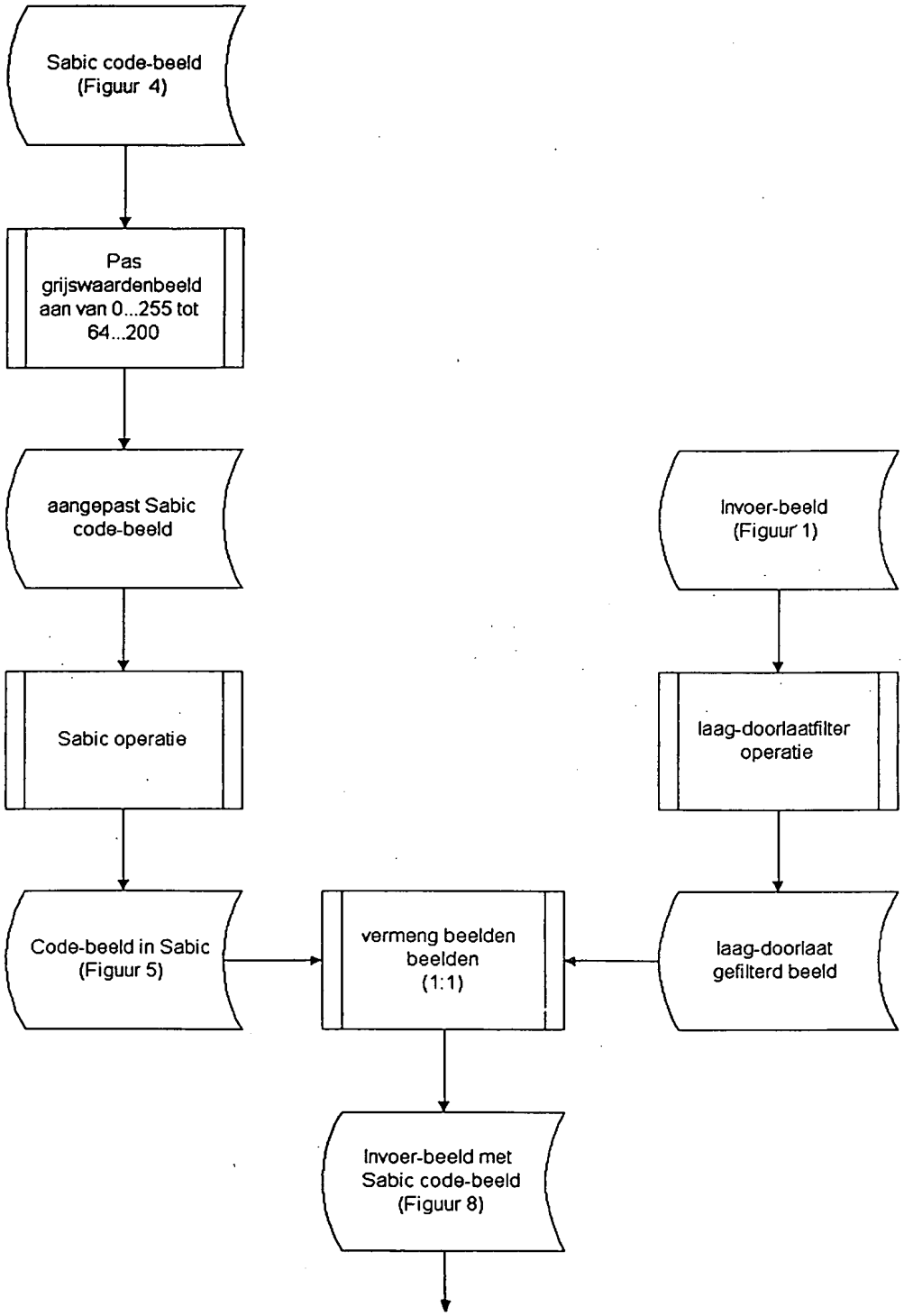
Sabic code-beeld (Figuur 4)
Pas grijswaardenbeeld aan van 0...255 tot 64...200
aangepast Sabic code-beeld
Sabic operatie
Code-beeld in Sabic (Figuur 5)
Invoer-beeld (Figuur 1)
laag-doorlaatfilter operatie
laag-doorlaat gefilterd beeld
vermeng beelden beelden (1:1)
Invoer-beeld met Sabic code-beeld (Figuur 8)

FIG. 27

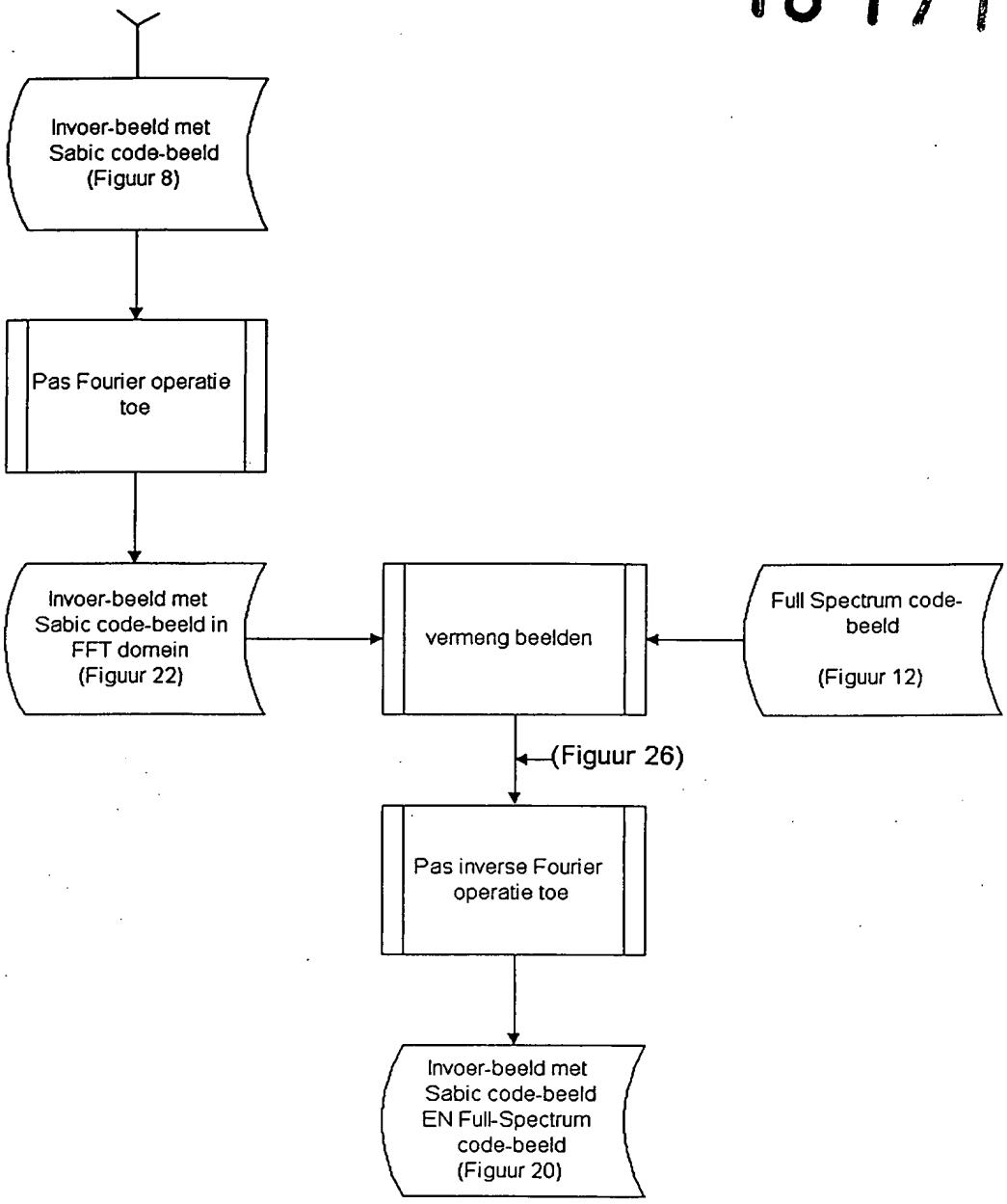

FIG. 27 (vervolg)